

**Notice of Allowability**

Application No.

10/057,521

Applicant(s)

TANAKA, NOBUYUKI

Examiner

Art Unit

Taghi T. Arani

2131

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--**

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 06/12/2006.
2. ☒ The allowed claim(s) is/are 1,4-10,13-19,22-28,31-37,40-46 and 49-55.
3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☒ All b) ☐ Some\* c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.  
**THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
- (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
- 1) ☐ hereto or 2) ☐ to Paper No./Mail Date \_\_\_\_\_.
- (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date \_\_\_\_\_
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date \_\_\_\_\_
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other \_\_\_\_\_

Taghi T. Arani  
Primary Examiner  
JANU 13 2006  
7/1/06

### **DETAILED ACTION**

1. The text of those sections of Title 35 U.S. Code not included in this section can be found in the prior office action.
2. The prior office actions are incorporated herein by reference. In particular, the observations with respect to claim language, and response to previously presented arguments.
3. Claims 2-3, 11-12, 20-21, 29-30, 38-39, 47-49, and 56-57 have been cancelled.
4. Claims 1, 10, 19, 22, 25-26, 28, 31, 34-35, 37, 40, 43-44, 46,49, 52-53 and 55 have been amended.
5. Claims 1, 4-10, 13-19, 22-28, 31-37, 40-46, 49-55, now re-numbered as claims 1-43 are pending.

### **EXAMINER'S AMENDMENT**

6. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. Seth Weinfeld on 07/07/2006.

Claim 55 has been amended as follows.

55. (Currently Amended) A computer readable [[record]] medium on which data has been [[recorded]] stored, said data comprising a data structure used for decrypting a subsequent portion of data based on a previous portion of data, said data structure comprising:

Art Unit: 2131

a first portion into which a first electronic watermark which contains a first encryption key has been inserted;

a second portion encrypted with said first encryption key;

an n-th electronic watermark which contains an n-th encryption key has been inserted into an n-th portion, where n is an integer larger than one; said data has an (n+1)-th portion encrypted with said n-th encryption key.

### **Response to Arguments**

7. Applicant's arguments filed 06/12/2006 in view of the above Examiner's Amendment have been fully considered and they are persuasive.

### **Allowable Subject matter**

8. Claims 1, 4-10, 13-19, 22-28, 31-37, 40-46, and 49-55 are allowed over prior art of record.

### **Examiner's Statement of Reasons for Allowance**

9. The following is an examiner's statement of reasons for allowance:

As per independent claims 1, 19, closest prior art of record directed to Yoshida teaches an encrypting apparatus and method using an encryption key contained in an electronic watermark, said apparatus comprising (Abstract, Fig. 12 and associated text):

generating means for generating a first electronic watermark which contains a first encryption key (Col. 12, lines 1-5, the decoding key is embedded as digital watermark) ;

electronic watermark inserting means for inserting said first electronic watermark containing said first encryption key into a first portion of data (Col. 12, lines 19-127, i.e. the

Art Unit: 2131

decrypting key is embedded in the imputed image corresponding to the head of audio block by the digital watermark embedding unit 1205 ); and

encrypting means for encrypting a second portion of said data with said first encryption key (Col. 12, lines 15-17, the encrypting unit 1203 enciphers each block of audio data by using the encrypting key generated by the key generating unit 1202).

Prior art of record singly or in combination fails to teach or fairly suggest wherein said electronic watermark generating means generates an n-th electronic watermark which contains an n-th encryption keys where n is an integer larger than one, said electronic watermark insertion means inserts said n-th electronic watermark into n-th portion of said data before said encryption means encrypts said n-th portion with an (n-1)-th encryption key and said encryption means encrypts an (n+1)-th portion of said data with said n-th encryption key. As recited in the amended claims 1, 19. Claim 37 is the corresponding computer program product embodied on a computer readable medium reciting the similar features as claims 1 and 19.

As per independent claims 10, 28, Yoshida teaches a decrypting apparatus and method using an encryption key contained in an electronic watermark, said apparatus comprising (Abstract, Fig. 13 and associated text):

electronic watermark detecting means for detecting a first electronic watermark from a first portion of data (Col. 12, lines 31-32, frame cutting-out unit 1301);

encryption key extracting means for extracting a first encryption key from said first electronic watermark (Col. 12, lines 46-48, the digital watermark extracting unit 1302 extracts the decoding key embedded as a signal watermark in the frame); and

Art Unit: 2131

decrypting means for decrypting a second portion of said data with said first encryption key (Col. 12, lines 49-55, the decoding unit 1304 decodes the audio block using decoding key).

Prior art of record singly or in combination fails to teach or fairly suggest “wherein said electronic watermark detecting means detects an  $n$ -th electronic watermark from an  $n$ -th portion of said data decrypted with an  $(n-1)$ -th encryption key by said decrypting means, where  $n$  is an integer larger than one, said encryption key extraction means extracts an  $n$ -th encryption key from said  $n$ -th electronic watermark. and said decrypting means decrypts an  $(n+1)$ -th portion of said data with said  $n$ -th encryption key” recited in independent claims 10 and 28. Claim 46 is the corresponding computer program product embodied on a computer readable medium reciting the similar features as claims 10 and 28.

Dependent claims 4-9, 13-18, 22-27, 31-36, 40-45 and 49-54 are allowed over prior art of record by virtue of their dependencies.

As per independent claim 55, Prior art of record singly or in combination fails to teach or fairly suggest an  $n$ -th electronic watermark which contains an  $n$ -th encryption key has been inserted into an  $n$ -th portion, where  $n$  is an integer larger than one; said data has an  $(n+1)$ -th portion encrypted with said  $n$ -th encryption key. That is prior art of record is silent in disclosing “decrypting a subsequent portion of the data based on a previous portion of data” wherein the decrypting key to decrypt the subsequent portion of the data is contained in a watermark inserted into the previous portion for  $n > 1$  as recited in the claim.

Art Unit: 2131

None of the prior art of record, either taken by itself or in any combination, would have anticipated or made obvious the invention of the present application at or before the time it was filed.

Any comments considered necessary by applicant must be submitted no later than payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

### **Conclusion**

10. Prior arts made of record, not relied upon:

Fang Bao, Multimedia Content Protection by Cryptography and Watermarking in Tamper-resistant Hardware, Proceedings of the 2000 ACM workshops on Multimedia Publisher, ACM Press, November 2000.


JP 10-164550, SCRAMBLE SYSTEM, BROADCASTING STATION DEVICE AND RECEIVING TERMINAL DEVICE.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Taghi T. Arani whose telephone number is (571) 272-3787. The examiner can normally be reached on 8:00-5:30 Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

  
Taghi T. Arani, Ph.D.  
Primary Examiner  
Art Unit 2131  
7/7/2006